Department of Homeland Security Daily Open Source Infrastructure Report for 02 November 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The News & Observer reports that all 81 emergency sirens within a 10−mile radius of North Carolina's Shearon Harris nuclear plant were inoperable Monday morning, October 30, and again Tuesday morning, October 31. (See item 1)
- CNN reports a Lufthansa plane headed to Frankfurt, Germany, with more than 300 people on board bumped an empty Continental Airlines Boeing 757 on Tuesday, October 31, at Newark Liberty International Airport. (See item 14)
- Reuters reports an explosive device blew out a thick, plate−glass window Tuesday evening, October 31, at the Silicon Valley, California, headquarters of PayPal, the online payments unit of eBay Inc. (See item 41)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *November 01, News & Observer (NC)* — **Siren test fails for Shearon Harris nuclear plant.** All 81 emergency sirens within a 10−mile radius of the Shearon Harris nuclear plant were inoperable Monday morning, October 30, and again Tuesday morning, according to Progress Energy, the plant's operator. The simultaneous failure of all sirens within the nuclear facility's

emergency planning zone was a first in the 19−year−history of the plant in southwestern Wake County, NC. The siren system at Shearon Harris is tested every 12 hours by a computer. The tests indicated that the device that signals all the sirens, called a "repeater," had failed to activate Monday and Tuesday, Progress Energy said in a notice to federal regulators. Progress Energy officials are repairing the malfunction. Plant operators can manually override the device to activate the sirens during an emergency.
Source: http://www.newsobserver.com/104/story/504909.html

2. *November 01, Reuters* — **FERC approves incentives to expand New England power grid.** The Federal Energy Regulatory Commission (FERC) this week authorized an increase in the return on equity for the owners of the ISO New England transmission grid to encourage needed expansion of the system. FERC said ratepayers would benefit because the present network leads to congestion costs and reliability problems, including involuntary load shedding. In a report this week, Fitch Ratings calculated congestion boosted New England consumer costs by about $788 million from 2000 to 2005. The expansion of the transmission infrastructure should help minimize these costs, the Commission said. The Commission determined that a base−level return on equity of 10.2 percent was appropriate.
Source: http://today.reuters.com/news/articleinvesting.aspx?type=governmentFilingsNews&storyID=2006−11−01T150419Z_01_N01327004_RTRIDST_0_UTILITIES−FERC−NEWENGLAND.XML

3. *October 31, Associated Press* — **Pipeline corrosion may be worse than first reported.** The Anchorage Daily News says corrosion along an oil pipeline at Prudhoe Bay is worse than first reported. The paper reports a test report on the three−mile pipeline shows it had more than 5,400 bad spots. Those spots include 176 places where corrosion might have chewed through half the pipe wall, or more. BP originally disclosed 16 anomalies in the pipe. In those areas, the company said, losses in wall thickness was between 70 and 81 percent. Repair or replacement is required if there is over an 80 percent loss.
Source: http://www.ktva.com/alaska/ci_4580412

4. *October 31, Utility Automation & Engineering* — **Dramatic changes needed to meet 2025 electricity needs: study.** The electric power system of 2025 will have to fuel everything from robotic home security guards to "tele−immersion" −− a next generation concept for telecommuting that mimics physical presence at a distance −− according to "Forecasting the Future of Electricity," released by the Galvin Electricity Initiative. To meet these needs, the U.S. electric power system must: Become highly efficient, from generation to end−use; adapt to allow consumers control of their energy service; provide reliable, digital quality power to all users who require it for everything from virtual schools to in−home small manufacturing; have the capacity to meet increasing plug loads as electricity replaces other uses of fossil fuels; and incorporate smart technologies that mitigate the effect of outages and attacks. The authors mapped out four potential pictures of what the U.S. will look like socially and economically in 2025; the technologies that will play substantive roles in each of these scenarios; and the energy supplies and innovations necessary to fuel them. The team then mapped out the required electric technology to fuel each and the overarching factors that must shape the electric power system of the future if it is to truly meet consumer need.
Source: http://uaelp.pennnet.com/display_article/276053/22/ARTCL/none/none/Dramatic_changes_needed_to_meet_2025_electricity_needs:_Galvin_study/

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *November 01, Orlando Sentinel* — **Ammonia leak prompts road closure.** One person suffered minor injuries Tuesday, October 31, following an ammonia leak at United States Cold Storage located at John Young Parkway and Shader Road in north Orange County, FL. The building was evacuated, and emergency workers shut down a section of Shader Road.
Source: http://www.orlandosentinel.com/news/local/orange/orl−cfbriefs01_1206nov01,0,417575.story?coll=orl−news−headlines−orange

6. *November 01, Associated Press* — **Employee killed at Tyson plant due to ammonia gas leak.** One worker was killed and another hospitalized after an ammonia gas leak at the Tyson Foods Inc. plant in South Hutchinson, KS. A 51−year−old man died and a 55−year−old man was hospitalized with chemical burns after the accident Tuesday, October 31. The men were refrigeration workers. They came in contact with ammonia gas after a refrigeration line broke outside of the main plant, Tyson spokesperson Gary Mickelson said in a written statement.
Source: http://www.kansas.com/mld/kansas/news/breaking_news/15901984.htm?source=rss&channel=kansas_breaking_news

7. *November 01, Associated Press* — **Ammonia gas leak in central China kills 1, forces evacuation of 20,000.** An ammonia gas leak at a factory owned by the Huangmailing Phosphorous Chemical Industry Group Company in central China killed one person, injured six and forced the evacuation of about 20,000 residents on Wednesday, November 1. The leak is the latest in a string of pollution incidents to hit China.
Source: http://www.kcbs.com/topic/ap_news.php?story=AP/APTV/National/a/i/China−AmmoniaLeak_a_i_−−−−−

[Return to top]

Defense Industrial Base Sector

8. *October 31, Reuters* — **Air Force said to seek $50 billion emergency funds.** The U.S. Air Force is asking the Pentagon's leadership for $50 billion in emergency funding for fiscal 2007 −− an amount equal to nearly half its annual budget, defense analyst Loren Thompson of the Lexington Institute said on Tuesday, October 31. The request is expected to draw criticism on Capitol Hill, where lawmakers are increasingly worried about the huge sums being sought "off budget" to fund wars, escaping the more rigorous congressional oversight of regular budgets. Thompson, who has close ties to U.S. military officials, said the big funding request was fueled by Deputy Defense Secretary Gordon England. England told the services in an October 25 memo to include the "longer war on terror," not just the wars in Iraq and Afghanistan, in their emergency requests. "This amount of money is so much bigger than the Air Force would normally request...it hints at a basic breakdown in the process for planning and funding war costs," said Thompson.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10

/31/AR2006103100621.html

[Return to top]

Banking and Finance Sector

9. *November 01, Guardian (UK)* — **Online ID theft booms as credit levels increase: study.** The average Briton is a tantalizing $108,000 target for identity scammers, according to a study. Thanks, in part, to a boom in the credit being offered by financial institutions and retailers, criminals who steal personal details are in for a bigger payday than ever before. But draining bank accounts and credit card balances amounts to only $17,000 of the total estimated value of a stolen identity. Scammers can make $76,000 by using an existing good credit rating to apply for more credit, while counterfeit passports and sham marriages are worth $6,000 apiece and a counterfeit driving license has a street value of $1,000. The report, commissioned by online identity management firm Garlik, estimated that ID thieves were fleecing more than 100,000 Britons a year, and this would increase to 200,000 in 2010. "Criminals are responsible for 75 percent of credit card fraud, and are rapidly moving into identity theft," said Tom Ilube of Garlik.
Note: Currency amounts in this article were converted from Euros to the nearest dollar.
Source: http://money.guardian.co.uk/news_/story/0,,1936252,00.html

10. *October 31, Associated Press* — **China approves anti−money laundering law.** China's top legislature approved a law Tuesday, October 31, strengthening the country's ability to combat money laundering as part of efforts to tackle financial crimes. The law requires financial institutions and some nonfinancial ones to keep detailed records of transactions and report large and suspicious transactions to authorities. The law defines money laundering crimes as those transactions related to drug trafficking, organized crime, and terrorism, as well as bribery and fraud. The law also stipulates that China will cooperate with other governments against money laundering. Chinese authorities will exchange intelligence related to suspected money laundering activities with foreign governments and international anti−money laundering organizations.
Source: http://biz.yahoo.com/ap/061031/apfn_china_money_laundering.h tml?.v=1

11. *October 30, Net Security* — **PandaLabs warns users of the mass−mailing of false job offers.** PandaLabs has detected the mass−mailing of messages with lucrative job offers, aimed at recruiting "mules". In Internet slang, "mules" are people used to launder stolen money, mainly originating from phishing or other online fraud. In this case, the message supposedly comes from an antique shop in Poland looking for sales reps to handle transactions outside the country. In exchange, the message claims the reps will receive lucrative commissions. According to PandaLabs, this is a large−scale attack, using at least ten Internet domains, and at least seven Web servers in countries including Korea, the U.S., Canada, Belgium, and Spain. In reality, the work of the mule involves receiving bank transfers and in exchange for commission on each operation, sending the money received to addresses provided by the criminals.
Source: http://www.net−security.org/secworld.php?id=4343

12. *October 26, Computing* — **Shift in motivation behind cybernet crime.** Silicon Valley FBI

agent Shena Crowe operates on the front line of computer fraud, and is aware of a definite shift in motivation behind Internet crime. There has yet to be a sentencing of anyone charged with masterminding a botnet, the latest and most virulent cyber threat, says Crowe. "The lack of reporting of cyber crime is one of the biggest challenges we face in law enforcement, and in effect we are pulling threads on a spider web and seeing what moves," she says. Yet from these small leads Crowe has discovered some large−scale profit−driven data thefts in the past year and a half. "The attacks are generally insider directed, carefully targeted and the methods are mostly combined," she says. "The insider direction is certainly becoming a major component in the crime we are seeing, and the data is then sold." The insiders are working as part of organized crime gangs whom she says present the most challenging development in Internet fraud. According to Crowe, to warrant a prosecution there has to be a $50,000 minimum in losses. That can be an accumulated loss between several victims, or in an international case, it must be about four times that figure.
Source: http://www.vnunet.com/computing/analysis/2167566/cyber−crime watch

[Return to top]

Transportation and Border Security Sector

13. *November 01, Boston Globe* — **Safety margin for Boston tunnel was smaller than most.** The Big Dig tunnel ceiling that collapsed in July was designed with a smaller margin of safety than other tunnel ceilings around the country, leaving nothing to prevent heavy concrete slabs from falling on a passing car when ceiling bolts fell out, according to a preliminary report sent to key federal officials on Tuesday, October 31. The Interstate 90 connector's drop ceiling was held up by steel hangers, which were suspended from bolts that had been glued into the tunnel roof. But there were no beams attaching the ceiling to the walls, and the ceiling was constructed with half as many ceiling bolts as in the original design. "No redundancy was built into the ceiling in the event the hangers failed," the National Transportation Safety Board (NTSB) states in its report. The report describes significant lapses by on the part of both the state government and private companies involved in the $14.6 billion Big Dig project. A lot of work remains to determine what happened and who is responsible. NTSB officials plan to interview more workers who built the ceiling, and lab analysts are testing the epoxy and how it was installed.
Source: http://www.boston.com/news/traffic/bigdig/articles/2006/11/01/safety_margin_for_tunnel_was_smaller_than_most_us_says/

14. *November 01, CNN* — **Planes bump at New Jersey airport.** A commercial plane with more than 300 people on board bumped an empty plane Tuesday, October 31, at Newark Liberty International Airport. A tip of the wing of Lufthansa Flight LH403, headed to Frankfurt, Germany, brushed the right winglet of a second plane, said Lufthansa spokesperson Jennifer Urbaniak. A wing on the Lufthansa Boeing 747 was damaged, she said. In a statement, Lufthansa said there were 291 passengers, three infants and 17 crewmembers on board. No injuries were reported. The passengers were taken off the plane. The second plane was an empty Continental Airlines Boeing 757, which was being relocated to a remote overnight parking spot "and was in a stationary position" when the contact occurred, the airline said in a statement. The Lufthansa flight was canceled. The Federal Aviation Administration will investigate, said Alan Hicks, spokesperson for the Port Authority of New York and New Jersey.
Source: http://www.cnn.com/2006/US/10/31/plane.crash/index.html

15. *November 01, Washington Post* — **Nationwide, airport waits get worse.** Nationwide, wait times during peak hours at airports increased to just over 13 minutes on average last week from about 11 minutes at the end of last month, according to the Transportation Security Administration (TSA). Two local airports surpassed those times. The average peak wait time at Washington Dulles International Airport rose to 25 minutes this month from about 14 minutes in September. Waits at Reagan National Airport were about five minutes longer this month than the 10−minute average TSA officials recorded in September. TSA officials said they thought the increased wait times stemmed from passengers carrying more bags onto airplanes since the gel and liquid ban was eased last month, forcing screeners to take more time to inspect luggage for potential explosives. Many passengers also remain confused about what they can take with them on planes, causing further delays as screeners throw out bottles of water and other banned items, they said Worried that wait times might lengthen during the holiday season, as inexperienced travelers go to airports, TSA officials said they were launching a publicity campaign to remind passengers about the revised restrictions. The TSA is also evaluating staffing levels and how travelers are informed about restricted items before they reach security checkpoints.
TSA Website: http://www.tsa.gov
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/30/AR2006103001208.html

16. *November 01, Reuters* — **Tampa airport reopens after partial evacuation.** Operations at Florida's Tampa International Airport returned to normal on Wednesday, November 1, after it was partially evacuated when a suspicious item was spotted, an airport spokesperson said. She said one concourse at the airport, used by JetBlue Airways Corp., AirTran Airways, Frontier Airlines Inc., and Continental Airlines, was shut down for a little over an hour before federal security officials gave the all−clear. She said the airport was fully operational again as of about 10:30 a.m. EST.
Source: http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyID=2006−11−01T163815Z_01_N01343877_RTRUKOC_0_US−USA−SECURITY−TAMPA.xml&WTmodLoc=USNewsHome_C2_domesticNews−5

17. *November 01, KTRK TV (TX)* — **Security breach forces shutdown at Bush Intercontinental Airport.** According to airport authorities, a man went through a security checkpoint at Terminal C this afternoon. Transportation Security Administration (TSA) screeners asked him to stop. The man didn't respond and kept going. TSA effectively shut down the terminal. Nobody was allowed in or out of the secured area, and the pedestrian train was stopped. As of 2:30pm, the situation had been resolved and everything was back to normal. The man was taken into custody.
Source: http://abclocal.go.com/ktrk/story?section=local&id=4717445

18. *October 31, Department of Transportation* — **Federal grants for Iowa, Minnesota, and South Carolina to help cut construction timeline for projects.** Iowa, Minnesota, and South Carolina will be the first states to each receive a $1 million grant under the Federal Highway Administration’s (FHWA) new “Highways for LIFE” program to help develop new approaches that can cut construction schedules in half, FHWA Administrator J. Richard Capka announced on Tuesday, October 31. The program encourages states to build roads faster, while making

them longer lasting and less costly to maintain. The program stresses innovation and promotes novel operational and contracting approaches that can shave time off construction projects. Capka noted that Iowa will use the grant to fund the reconstruction of an interchange in Council Bluffs using prefabricated bridge sections that can be made away from the roadway and installed overnight, sparing drivers months of onsite roadwork. Minnesota will reconstruct a portion of Highway 36 in Minneapolis/St. Paul using a full−road closure for five months to complete the project faster. South Carolina will use a "no excuses" clause in a construction contract for meeting the specified completion date for a bridge project in Kingstree.
Source: http://www.dot.gov/affairs/fhwa1306.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

19. *October 31, Ag Professional* — **Kansas State researcher finds new wheat virus.** Kansas State University scientist Dallas Seifers has found a virus never before detected in wheat. Although the virus was found in multiple locations around the state last spring, including university fields and privately−owned land, there was no indication that it had a significant yield impact on the 2006 wheat crop, he said. The virus, which Seifers is calling triticum mosaic virus, seems to have affected cultivars that have been developed for their resistance to wheat streak mosaic, he said. There are still many unknowns about the disease, Seifers said, including what impact it might have on yields in coming years, how widespread it was in 2006 and what sort of weather conditions it favors.
Source: http://www.agprofessional.com/show_story.php?id=43910

20. *October 31, Associated Press* — **Another herd found infected with bovine tuberculosis.** Bovine tuberculosis has been found in a seventh beef cattle herd in Roseau and Beltrami counties of northwestern Minnesota, the Minnesota Board of Animal Health said Tuesday, October 31. The U.S. Department of Agriculture is working out the details of destroying the animals in the newest herd and compensating the owner. While officials are tracking the movement of animals in and out of the operation, the board said the herd is small and has had minimal movement. The case turned up as part of a program that calls for testing all herds within 10 miles of an infected beef herd or an infected white−tail deer.
Source: http://www.twincities.com/mld/twincities/news/15893643.htm

21. *October 27, Capital Press* — **Virus stunts onions in Oregon and Idaho.** Treasure Valley onion growers in Malheur County, OR, and southwestern Idaho suffered their heaviest losses ever this year due to a virus spread by onion thrips. Iris yellow spot virus significantly reduced sweet Spanish onion size and thus overall yields in the famous growing region, said Oregon State University Malheur County Extension agent Lynn Jensen. Jensen said this is the worst pest−related setback he's seen in onions in his 20 years in Malheur County. Yellow spot virus

was first detected in the U.S. in 1989 in Treasure Valley, and has been gradually taking its toll on onion crops there ever since. During the last few years, except for 2004, it has been particularly damaging. Other than preventing plants from growing normally and producing a large quantity of colossal and super colossal onions, the virus, which is spread to plants when thrips feed on them, does no damage to the onions themselves, Jensen said. Yellow spot virus has been a problem in other U.S. onion−growing areas and then subsided, Jensen said. "Eastern Oregon and Idaho seem to be the hardest−hit areas."
Source: http://www.capitalpress.info/main.asp?SectionID=67&SubSectionID=792&ArticleID=28313

[Return to top]

Food Sector

22. *October 31, Associated Press* — **Salmonella outbreak appears over, health official says.** A federal official says the salmonella outbreak that sickened dozens of people in 19 states appears to be over, while investigators remain unsure how it began. There have been no deaths, but 171 people have fallen sick. Officials revised downward the tally by one case on Tuesday, October 31, following further investigation. The Food and Drug Administration says reports of illness peaked in late September, suggesting the outbreak is now over.
Source: http://www.abc6.com/engine.pl?station=wlne&id=22636&template=breakout_story_local_news.shtml&dateformat=%25M+%25e,%25Y

[Return to top]

Water Sector

23. *October 31, Tucson Citizen (AZ)* — **Tucson Convention Center leaking tainted water for three months.** A series of water leaks in the ventilation system that serves the Tucson Convention Center and Police and Fire department headquarters has been pouring 1,000 gallons of water tainted with a suspected carcinogen each day into the ground nearby. The leaks, in the pipes that carry water for heating and cooling to nearby city buildings, were discovered in August, but have not been pinpointed and may have existed since 2003. As many as 29,000 gallons of water treated with sodium nitrite were lost every month, said Ron Lewis, director of the city's General Services Department. Sodium nitrite, a common food additive, is used to prevent pipes from corroding. When combined with oxygen, it becomes sodium nitrate, said Nancy Petersen, deputy director of the city's Environmental Services Department. High levels of the compound in drinking water have been linked to cancer and can hamper infants' ability to get oxygen into the bloodstream, she said. Officials said there are no city wells in the area and the drinking water downtown is piped from other areas of town.
Source: http://www.tucsoncitizen.com/daily/local/31017.php

[Return to top]

Public Health Sector

24. *November 01, Washington Post* — **CDC shifts vaccine−data focus.** Federal health officials have decided to forgo gathering detailed data on whether children in 22 big cities are receiving recommended immunizations and instead will survey teenagers, who are the target of several new vaccines. The decision is drawing protests from local health officials, who say the soon−to−be−lost information is essential to their efforts to make sure that infants and toddlers, many from poor families, are protected against childhood infections. Officials at the Centers for Disease Control and Prevention (CDC) who made the decision said they are reluctantly choosing between two worthy goals. "It was really a very, very difficult decision. But we think we have to have information about adolescents because it is such a growth area," said Lance Rodewald, director of the CDC immunization services division. Historically, most vaccines have been administered to infants and young children and only few to adolescents and teenagers, but that is changing. Under recently approved guidelines, pre−teenage girls should receive the new human papilloma virus vaccine; college freshmen should have the meningococcal meningitis vaccine; and most teenagers should receive boosters for tetanus, diphtheria and pertussis, as well as the chickenpox vaccine if they did not receive it as children.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/31/AR2006103101302.html

25. *October 31, Center for Infectious Disease Research & Policy (MN)* — **Pandemic vaccine rationing proposal favors the young.** In a worst−case influenza pandemic, without enough vaccine for everyone, who should stand closer to the front of the line: a 25−year−old water utility worker or a healthy 75−year−old? Public health officials may have to make difficult decisions such as this, and a Minnesota health ethics group, in publishing recommendations about pandemic vaccine allocation, hopes to get conversations going now, rather than during a crisis. The vaccine allocation recommendations released last week by the Minnesota Center for Health Care Ethics (MCHCE) look much different from the ones proposed by the federal government. The vaccine rationing recommendation in federal pandemic plan is aimed at saving the most lives, and might favor the healthy 75−year−old over the 25−year−old utility worker. The Minnesota group's approach is designed to prevent not only deaths due to influenza, but also deaths related to public infrastructure breakdowns. It is weighted toward those whose immune systems are more likely to respond strongly to a pandemic flu vaccine. As such, it would put the 25−year−old utility worker ahead of the 75−year−old.
MCHCE recommendations: http://www.stolaf.edu/mnethx/PanFluReport.pdf
Source: http://www.cidrap.umn.edu/cidrap/content/influenza/panflu/ne ws/oct3106ethics.html

26. *October 31, Center for Infectious Disease Research & Policy (MN)* — **WHO: H5N1 cases in Turkey targeted children, youth.** A recent World Health Organization (WHO) report on 10 of the 12 confirmed H5N1 avian influenza cases that occurred in Turkey last winter adds to evidence that children and youth may be particularly susceptible to the infection. The disease struck only children younger than 16, even though their parents had probably been exposed to the same probable source of infection, infected poultry, according to the Friday, October 27, issue of the World Health Organization's (WHO) Weekly Epidemiological Record. "To some extent, this reflects the same age distribution observed globally, where 50.5 percent of cases occurred among people aged WHO report: http://www.who.int/wer/2006/wer8143.pdf
Source: http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/oct3106turkey.html

27. *October 31, Canadian Press* — **New bird flu variant doesn't seem to pose greater human health risk: WHO.** The emergence of a new variant of H5N1 avian flu viruses doesn't appear to raise or lower the risk the virus poses to humans, officials of the World Health Organization (WHO) and the Food and Agriculture Organization said Tuesday, October 31. Representatives of the United Nations agencies charged with animal and human health issues held a teleconference Tuesday to discuss the discovery of the new subgroup of viruses. The new variant, called a Fujian−like virus, was reported Monday, October 30, in the scientific journal The Proceedings of the National Academy of Sciences. But the pattern of human cases with these viruses is similar to that seen with viruses spreading in Indonesia, or those that caused human infections in Vietnam in 2004 and 2005, said Michael Perdue of the WHO. The variant is responsible for recent human cases in China and Thailand. "If you look at the mortality rate and the disease, the Fujian−strain infections are no different," said Perdue, a senior scientist with the WHO's global influenza program. "So there's no reason to lead us to believe that this sublineage is acting any differently than any of the other sublineages in terms of affecting humans."
Source: http://www.cbc.ca/cp/health/061031/x103112.html

28. *October 31, Cornell University* — **Findings could foil two potential bioterror agents.** Two lethal and easily transmitted viruses −− both potential bioterror agents −− may soon be much less dangerous, thanks to research led by scientists at Weill Cornell Medical College in New York City. Hendra and Nipah viruses are related, newly recognized zoonotic viruses that can spread from their natural reservoir in fruit bats to larger animals −− including pigs, horses and humans. The mode of transmission isn't clear, but is thought to be relatively easy −− either by close contact with an infected host or by breathing in the microscopic pathogens. Infection often leads to a fatal encephalitis, and there is currently no effective treatment against these illnesses. However, researchers at Weill Cornell say that by tweaking a peptide (protein) related to a third pathogen, parainfluenza virus, they may be able to prevent Hendra and Nipah virus from infecting human cells. The findings are published in this month's issue of the Journal of Virology.
Abstract: http://jvi.asm.org/cgi/content/abstract/80/19/9837?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&author1=moscona%2C+A.&titleabstract=Viral+Peptide+Prevents+Deadly+Hendra%2C+Nipah+Viruses+from+Infecting+Cells&searchid=1&FIRSTINDEX=0&fdate=10/1/2006&resourcetype=HWCIT
Source: http://news.med.cornell.edu/wcmc/wcmc_2006/10_31a_06.shtml

29. *October 27, National Science Foundation* — **Ecologists to study West Nile virus, malaria, bird flu, and other infectious diseases.** Over the past 20 years, unprecedented changes in biodiversity have coincided with the emergence and re−emergence of numerous infectious diseases around the world. To address this problem, the National Science Foundation (NSF) and the National Institutes of Health have announced funding for eight projects under the Ecology of Infectious Diseases (EID) program, a multi−year, joint−agency effort now in its seventh year of funding. "Researchers supported in the EID program are advancing basic theory related to infectious diseases," said James Collins, NSF Assistant Director for Biological Sciences, "and applying that knowledge to improve our understanding of how pathogens spread through populations at a time of increasing global change." Interdisciplinary projects funded through the EID program will study how large−scale environmental events alter the risks of

viral, parasitic and bacterial diseases emerging in humans and animals.
Source: http://www.nsf.gov/news/news_summ.jsp?cntn_id=108141&org=NSF &from=news

[Return to top]

Government Sector

30. *November 01, Washington Post* — **Boy, 15, arrested after 'bottle bomb' blows up near school bus.** A 15−year−old Rockville, MD, student was arrested Tuesday afternoon, October 31, after a homemade "bottle bomb" he was about to bring onto a school bus exploded as a teacher discarded it, Montgomery County Fire and Rescue Service officials said. A teacher at Mark Twain School in Rockville who saw something suspicious approached the student −− whom authorities did not identify because he was charged as a juvenile −− as he was getting ready to board a school bus. As the teacher seized the two−liter bottle, its contents were activated by the movement, leading to an explosive chemical reaction. No one was injured. Most students who attend Mark Twain have special education needs, such as learning disabilities and behavioral problems.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/31/AR2006103101195.html

31. *November 01, Associated Press* — **Traffic briefly blocked near White House.** Traffic was blocked off several streets near the White House briefly Tuesday evening, October 31, after a man outside the Treasury Department falsely claimed to be carrying an explosive, the Secret Service said. No explosive was found and the man was taken into custody for a mental evaluation, Secret Service spokesperson Kim Bruce said. He was not immediately charged and his identity was withheld pending the outcome of the evaluation. Applying standard security measures, the Ellipse south of the White House, 15th Street between Pennsylvania Avenue and Constitution and E Street between 15th and 17th streets were closed to vehicles and pedestrians until 10:49 p.m., Bruce said.
Source: http://www.usatoday.com/news/nation/2006−11−01−white−house−t hreat_x.htm

[Return to top]

Emergency Services Sector

32. *October 31, WALB−TV (GA)* — **New dispatch program could save lives.** In Valdosta, GA, the police department is implementing closest car dispatch, a program they believe will shave precious moments off their response time. "That means if you call 911 and somebody's breaking into your house, instead of the old method where the dispatcher will send a beat officer or officers in your area, the dispatcher can look to see marked and unmarked cars and the closest one gets the call," said Captain Brian Childress of the Valdosta Police. The department has placed Automated Vehicle Locator computers in all patrol cars. These computers allow dispatchers to see the location of each marked and unmarked car and send the five closest cars to the caller's location.
Source: http://www.walb.com/Global/story.asp?S=5614809&nav=5kZQ

33. *October 31, Bloomberg* — **Chile's quake−frightened citizens train for tsunamis.** Chile, one of the world's most earthquake−prone nations, is conducting its biggest drill ever along the country's populated coast, training residents to survive a temblor large enough to trigger a tsunami. Officials in the seaside city of Valparaiso are deploying audio speakers on Tuesday, October 31, to simulate the rumble of a quake and the rush of a tidal wave sweeping through the streets, said Jorge Enriquez, chief of civil protection at the state's National Emergency Office. Actors, some yelling and weeping, will add a sense of reality, Enriquez said. During the mock quake, residents of Valparaiso and the seaside town of Concon will learn the best routes to escape to higher ground from an incoming wave, to move on foot to avert traffic jams, leave roadways clear for the disabled, and to stay calm, Enriquez said. About 4,000 to 5,000 people will participate in the drill in Valparaiso, involving the public on a large scale for the first time rather than just police, fire, and emergency responders, said Guillermo de la Maza, the provincial director of civil protection and emergencies.
Source: http://www.bloomberg.com/apps/news?pid=20601101&sid=aCMMUUlNP3so&refer=japan

[Return to top]

Information Technology and Telecommunications Sector

34. *November 01, eWeek* — **Microsoft confirms critical Visual Studio zero−day.** An "extremely critical" vulnerability in Microsoft Visual Studio 2005 could put users at risk of remote code execution attacks, the company confirmed Wednesday, November 1. The software maker issued a security advisory with pre−patch workarounds and warned that the flaw is already being used in zero−day attacks.
Microsoft Security Advisory: http://www.microsoft.com/technet/security/advisory/927709.mspx
Source: http://www.eweek.com/article2/0,1895,2048968,00.asp

35. *November 01, Associated Press* — **ICANN: Multi−lingual system could permanently break the Internet.** The body that oversees global Internet functions warned Wednesday, November 1, that a mistake in a creating multi−lingual address system could "permanently break the Internet." The Internet Corporation for Assigned Names and Numbers (ICANN) made the warning at a United Nations−organized conference on the future of the Internet being held in Greece. More multi−lingual Internet is a key issue at the forum, with future Web growth predicted in developing countries where the Latin alphabet is often unfamiliar. "ICANN expects that these final tests and discussions will reach a resolution by the end of 2007," CEO Paul Towney said in a statement. "But this is no simple task. If we get this wrong we could very easily and permanently break the Internet." Experts at the forum have also warned that mixed use of alphabets in Internet addresses could allow cybercriminals a greater opportunity to post imitation Websites typically created for illegally collecting personal banking details. The four−day Internet Governance Forum ends Thursday, November 2.
Source: http://news.yahoo.com/s/ap/20061101/ap_on_hi_te/greece_un_internet_governance

36. *October 31, U.S. Department of Defense* — **Department of Defense: Extremists use sophisticated Internet assaults.** A group calling itself “Electronic Jihad” has begun an Internet program that bombards Websites it considers anti−Islamic with spam messages until they shut

down. It is the most sophisticated Web−based program known to be used by terrorists to date. Electronic Jihad are “Internet activists” who “support the Lebanese and Palestinian resistance,” and who claim that “thousands...are participating” in the attacks, according to Pentagon policy reports. These activists are promoting their cause on various Websites and calling on other militant radical Islamic groups to join them. Government and business Websites around the globe could be threatened by these tactics. In addition, Pentagon policy experts warn that participating in Web−based assaults are low risk for groups wanting to support the militant Islamic cause and could lead to more extreme actions in the future.
Source: http://www.defenselink.mil/home/dodupdate/enemy−update/docs/10−31−06_Nature_of_Enemy.pdf

37. *October 31, Federal Times* — **Hackers −− from locals to Chinese −− challenge data security.** From the Chinese government to homegrown hackers, groups are increasingly targeting agencies’ networks, data security experts claim. “The Chinese are in half of your agencies’ systems,” Alan Paller, research director of the SANS Institute, told attendees Monday, October 30, at the Executive Leadership Conference. Paller cited 2005 reports that hackers using servers in China stole designs for an aviation mission−planning system for Army helicopters, and, on one night in 2004, found vulnerabilities in computers at the Defense Information Systems Agency, the Naval Ocean Systems Center in San Diego, the Army Information Systems Engineering Command at Fort Huachuca, AZ, and the Army Space and Strategic Defense Installation in Huntsville, AL. Officials believe the attacks were sponsored by the Chinese government. Paller argued that many information security metrics established by the Federal Information Security Management Act do not measure how well agencies protect data. Agencies must report the number of systems for which they complete reports on security vulnerabilities, but most reports are written by consultants and never read by top managers, Paller said. Agencies are also required to count the number of officials who complete security awareness training, but do not have to measure what skills they acquired, he said.
Source: http://federaltimes.com/index.php?S=2323081

38. *October 31, Security Focus* — **Sophos Antivirus multiple denial−of−service vulnerabilities.** Sophos Antivirus is prone to multiple denial−of−service vulnerabilities. A remote attacker may trigger these issues to deny service to legitimate users.
Vulnerable: Sophos Anti−Virus 5.2.1; Sophos Anti−Virus 5.2; Sophos Anti−Virus 5.0.4; Sophos Anti−Virus 5.0.2; Sophos Anti−Virus 5.0.1; Sophos Anti−Virus 4.7.2; Sophos Anti−Virus 4.7.1; Sophos Anti−Virus 4.5.12; Sophos Anti−Virus 4.5.11; Sophos Anti−Virus 4.5.4; Sophos Anti−Virus 4.5.3; Sophos Anti−Virus 5.1; Sophos Anti−Virus 4.05; Sophos Anti−Virus 4.04.
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/20816/references

39. *October 30, IDG News Service* — **Tricky new malware unnerves security vendors.** A tricky malicious program has become more prevalent in spam, but experts don't know what its creators plan to do with it. Many vendors are rating the malware −− called "Warezov," "Stration" and "Stratio" −− as a low risk. But they also say that it is tricky to deal with. The malware is a mass−mailing worm that affects machines running Microsoft Corp.'s Windows operating system. When the malware infects a computer, it sends itself out again to other e−mail addresses found on the computer. The code is then capable of downloading new

versions of itself as frequently as every 30 minutes from a batch of Websites, said Mikko Hypponen, chief research officer at F−Secure Corp. However, analysts don't know how the new code is generated.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=networking&articleId=9004601&taxono myId=16

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	15281 (−−−), 4662 (eDonkey2000), 6881 (bittorrent), 1026 (win−rpc), 13886 (−−−), 4672 (eMule), 6346 (gnutella−svc), 445 (microsoft−ds), 50001 (−−−), 65530 (WindowsMite) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

40. *November 01, Associated Press* — **Woman arrested after Reno hotel fire kills six.** A woman was arrested Wednesday, November 1, on arson and murder charges after a fire swept through a three−story hotel in Reno, NV's downtown casino district, killing six people and injuring dozens of others. Police Chief Michael Poehlman said the 47−year−old woman set fire to a mattress in her room at the Mizpah Hotel. Officials were still trying to determine a motive. Police estimated that when the fire started, 60 to 80 people were inside the 84−year−old brick building, a primarily residential hotel that had been recently renovated. The blaze quickly engulfed the hotel's north wing, which covers most of a city block just east of Harrah's. None of the downtown high−rise hotel−casinos was threatened, Poehlman said. A few residents jumped to safety from windows as the hotel burned. Others were rescued by firefighters with ladders and city workers who were in the area with a cherry picker. About 30 people were injured, some from jumping. The building's roof collapsed in the blaze. The Mizpah was built in 1922 and added to the National Register of Historic Places in 1984.
Source: http://www.usatoday.com/news/nation/2006−11−01−reno−fire_x.h tm

41. *November 01, Reuters* — **Explosive device shatters window at Paypal HQ.** An explosive device blew out a thick, plate−glass window Tuesday evening, October 31, at the Silicon Valley headquarters of PayPal, the online payments unit of eBay Inc. No injuries resulted when what local fire officials said was an explosive device shattered a six−foot−square window on the ground floor of the four−story building in San Jose, CA. The explosion occurred outside a building exit. Investigators were still trying to determine the nature of the device. "Whatever it was, it disintegrated," San Jose Fire Department Capt. Jose Guerrero said. About 45 employees were working in the PayPal offices when the explosion occurred, eBay spokesperson Hani Durzy said. "We have no reports concerning threats," Durzy said. "We are still investigating and we are working with local and federal authorities." The PayPal offices, where 1,900

employees work, were closed Wednesday, November 1, while police conducted an investigation.
Source: http://news.yahoo.com/s/nm/20061101/tc_nm/crime_ebay_explosi on_dc

[Return to top]

General Sector

42. *November 01, Associated Press* — **Man arrested for California arson fires; fifth firefighter dies from burns.** Authorities arrested a man Tuesday, October 31, who is suspected of intentionally starting two wildfires this summer and is considered a person of interest in a blaze started last week that has killed five firefighters. Raymond Lee Oyler, 37, of Beaumont, CA, was arrested on two counts of arson related to wildfires in June, the Riverside County Sheriff's Department said in a statement. Oyler was not named as a suspect in the wildfire that started last week and roared across more than 60 square miles. Investigators interviewed Oyler on Friday and then searched his home on Monday, the sheriff's department said. No other details were released. As part of the investigation, authorities said they sifted through hundreds of tips and interviewed previously convicted arsonists who live in the Cabazon area. Assisting in the investigation were the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Federal Bureau of Investigation. The reward for information leading to an arrest topped $500,000.
Source: http://www.usatoday.com/news/nation/2006−10−31−socal−fire_x. htm

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.